CLAIMS

What is claimed is:

1. A method comprising:

determining one or more packet tag values of one or more newly received packets over a connection has changed from previously received packet tag values; and

modulating the policy applied to the one or more packets in response to identifying the change in the one or more packet tag values using a hysteresis response.

2. An apparatus comprising:

an intra-flow policy modulator to modulate policies applied to packets of a connection using a hysteresis response, wherein the intra-flow policy modulator comprises

a classification module to receive incoming traffic, assign a traffic class to the incoming traffic based on a packet tag in the incoming traffic, and vary the traffic class applied to a connection in response to receipt of a different packet tag; and

a policy module to assign a policy to the incoming traffic based on the assigned traffic class and to control outgoing traffic based on the assigned policy for the incoming traffic.

3. The apparatus defined in Claim 2 wherein the intra-flow policy modulator performs the hysteresis response when varying traffic classes in response to the different packet tag having a higher priority.

4. The apparatus defined in Claim 2 wherein the connection comprises a TCP connection.

5. The apparatus defined in Claim 2 wherein the classification module identifies a service type associated with the incoming packet and determines whether to change the traffic class assignment based on the service type.

6. The apparatus defined in Claim 5 wherein the classification module determines whether to change the traffic class assignment is based on the service type associated with the incoming packet.

7. The apparatus defined in Claim 2 wherein the classification module uses a mapping of tag bits to its traffic class and a policy.

8. The apparatus defined in Claim 7 wherein the classification module changes the mapping between at least one of the plurality of tag bits and its traffic class and policy based on a set of classification change rules.

9. The apparatus defined in Claim 2 wherein the policy module applies a policy to the incoming traffic based on assigned traffic class and controls outgoing traffic based on the assigned policy for the incoming traffic.

10. The apparatus defined in Claim 9 wherein the policy manager controls the outgoing traffic by providing less importance to traffic having a first type of tag and more importance to traffic having a second type of tag using the assigned policy for the incoming traffic.

11. A method comprising:

mapping policies to traffic classes associated with flows of packets in a network;

modulating assignment of traffic classes to individual connections in the network based on one or more changes in packet tags using a hysteresis response.

12. An apparatus comprising:

means for mapping policies to traffic classes associated with flows of packets in a network;

means for modulating assignment of traffic classes to individual connections in the network based on one or more changes in packet tags using a hysteresis response.

13. A method comprising:

assigning a first traffic class to incoming traffic within a connection based on a first ICA Virtual Channel Tag of a first packet in the incoming traffic; and

changing the traffic class based on a second ICA Virtual Channel Tag of a second packet within the connection in the incoming traffic to reclassify the connection in response to changes in packet tags.

14. The method defined in Claim 13 wherein the incoming traffic includes a sequence of packets in order for which out of order delivery degrades performance for the single connection.

15. The method defined in Claim 13 wherein the connection comprises a TCP connection.

16. The method defined in Claim 13 further comprising varying policies applied to the connection.

17. The method defined in Claim 13 further comprising determining a relative importance of different types of tagged traffic within one TCP connection.

18. The method defined in Claim 13 further comprising:

identifying a service type associated with the incoming packet; and

determining whether to change the traffic class assignment based on the service type.

19. The method defined in Claim 18 wherein determining whether to change the traffic class assignment is based on the service type associated with the incoming packet.

20. The method defined in Claim 18 further comprising:

checking for a policy for the traffic class;

applying the policy to the connection.

21. The method defined in Claim 13 further comprising mapping a plurality of packet tags to a traffic class and a policy.

22. The method defined in Claim 21 further comprising changing a mapping between at least one of the plurality of packet tags and its traffic class and policy based on a set of classification change rules.

23. The method defined in Claim 13 further comprising:

applying a policy to the incoming traffic based on assigned traffic class; and

controlling outgoing traffic based on the assigned policy for the incoming traffic.

24. The method defined in Claim 23 wherein the controlling of the outgoing traffic includes providing less importance to traffic having a first type of ICA Virtual Channel Tag and more importance to traffic having a second type of ICA Virtual Channel Tag using the assigned policy for the incoming traffic.

25. The method defined in Claim 13 wherein the incoming traffic comprises print traffic.

26. The method defined in Claim 13 wherein the connection comprises a Citrix connection, and further comprising:

specifying subclasses within a Citrix ICA service that correspond to a mapping of the traffic class to the Virtual Channel Traffic Tag value;

assigning a policy to each of the subclasses;

recognizing a change in the virtual channel tag value while receiving packets in the connection; and

switching the traffic class to another in response to the change in the virtual channel tag value.

27. The method defined in Claim 13 wherein the connection comprises a Citrix connection, and further comprising:

receiving a packet having a virtual channel priority tag numerically larger than the virtual channel tag of a previous packet;

switching the first traffic class to a new traffic class assigned to the largest priority tag value.

28. The method defined in Claim 27 further comprising

remaining in the new traffic class for a period of time; and

switching to the first traffic class assigned to next largest priority tag value after a predetermined time.

29. An apparatus comprising:

a classification module to receive incoming traffic and to assign a first traffic class to the incoming traffic based on a ICA Virtual Channel Tag in the incoming traffic, wherein the classification module varies the traffic class applied to a connection in response to receipt of a different ICA Virtual Channel Tag; and

a policy module to assign a policy to the incoming traffic based on the assigned traffic class and to control outgoing traffic based on the assigned policy for the incoming traffic.

30. The apparatus defined in Claim 29 wherein the incoming traffic includes a sequence of packets in order for which out of order delivery degrades performance for the single connection.

31. The apparatus defined in Claim 29 wherein the connection comprises a TCP connection.

32. The apparatus defined in Claim 29 wherein the classification module identifies a service type associated with the incoming packet and determines whether to change the traffic class assignment based on the service type.

33. The apparatus defined in Claim 32 wherein the classification module determines whether to change the traffic class assignment is based on the service type associated with the incoming packet.

34. The apparatus defined in Claim 29 wherein the policy module assigns a policy to each traffic class.

35. The apparatus defined in Claim 29 wherein the classification module maps packet tags to a traffic class and a policy.

36. The apparatus defined in Claim 35 wherein the classification module changes a mapping between at least one of the plurality of packet tags and its traffic class and policy based on a set of classification change rules.

37. The apparatus defined in Claim 29 wherein the policy module applies a policy to the incoming traffic based on assigned traffic class and controls outgoing traffic based on the assigned policy for the incoming traffic.

38. The apparatus defined in Claim 37 wherein the policy manager controls the outgoing traffic by providing less importance to traffic having a first type of ICA Virtual Channel Tag and more importance to traffic having a second type of ICA Virtual Channel Tag using the assigned policy for the incoming traffic.

39. The apparatus defined in Claim 29 wherein incoming traffic comprises print traffic.

40. The apparatus defined in Claim 29 wherein the packet tag comprises a priority tag.

41. An apparatus comprising:

means for assigning a first traffic class to incoming traffic within a connection based on a first ICA Virtual Channel Tag of a first packet in the incoming traffic; and

means for changing the traffic class based on a second ICA Virtual Channel Tag of a second packet within the connection in the incoming traffic, such that the connection is reclassified in response to changes in packet tags.

42. An article of manufacture having a machine-readable medium with executable instructions thereon which, if executed by a computing system, causes the computing system to:

assign a first traffic class to incoming traffic within a connection based on a first ICA Virtual Channel Tag of a first packet in the incoming traffic; and

change the traffic class based on a second ICA Virtual Channel Tag of a second packet within the connection in the incoming traffic such that the connection is reclassified in response to changes in packet tags.

43. A method comprising:

receiving a new packet on a network connection;

determining whether to delay transmission of the new packet to a location to avoid subsequent retransmission to the location; and

transmitting the new packet to the location on the network connection at a time selected to avoid the subsequent retransmission to the location.

44. The method defined in Claim 43 wherein the network connection is a TCP connection.

45. The method defined in Claim 43 further comprising transmitting one or more additional packets received after receiving the new packet prior to transmitting the new packet.

46. The method defined in Claim 43 wherein the network connection comprises a shared communication link.

47. A method comprising:

checking whether a first priority associated with a new incoming packet of a TCP connection is greater than a second priority associated with a previous incoming packet of the TCP connection;

transmitting the new incoming packet at the first priority if the first priority is not greater than the second priority;

determining whether the new incoming packet will arrive substantially out of order in that the incoming packet will arrive before the previous incoming packet such that retransmission of the previous incoming packet or the new incoming packet will result;

transmitting the new incoming packet at the first priority if the new incoming packet is not determined to arrive substantially out of order with respect to the previous incoming packet; and

transmitting the new incoming packet at the second priority if the new incoming packet is determined to arrive substantially out of order with respect to the previous incoming packet.

48. A bandwidth manager comprising:

a TCP conditioner-based policy modulator to modulate policies applied to packets of a TCP connection based on a determination as to whether each of the packets will arrive substantially out of order, wherein the TCP conditioner-based policy modulator comprises

a classification module to receive incoming traffic, assign a traffic class to the incoming traffic based on a packet tag in the incoming traffic, and vary the traffic class applied to a connection in response to receipt of a different packet tag; and

a policy module to assign a policy to the incoming traffic based on the assigned traffic class and to control outgoing traffic based on the assigned policy for the incoming traffic.

49. The bandwidth manager defined in Claim 48 wherein the intra-flow policy modulator performs the hysteresis response when varying traffic classes in response to the different packet tag having a higher priority.

50. The bandwidth manager defined in Claim 48 wherein the classification module identifies a service type associated with the incoming packet and determines whether to change the traffic class assignment based on the service type.

51. The bandwidth manager defined in Claim 50 wherein the classification module determines whether to change the traffic class assignment is based on the service type associated with the incoming packet.

52. The method defined in Claim 48 wherein the classification module uses a mapping of tag bits to its traffic class and a policy.

53. The method defined in Claim 52 wherein the classification module changes the mapping between at least one of the plurality of tag bits and its traffic class and policy based on a set of classification change rules.

54. The bandwidth manager defined in Claim 48 wherein the policy module applies a policy to the incoming traffic based on assigned traffic class and controls outgoing traffic based on the assigned policy for the incoming traffic.

55. The bandwidth manager defined in Claim 54 wherein the policy manager controls the outgoing traffic by providing less importance to traffic having a first type of tag and more importance to traffic having a second type of tag using the assigned policy for the incoming traffic.

56. A apparatus comprising:

means for checking whether a first priority associated with a new incoming packet of a TCP connection is greater than a second priority associated with a previous incoming packet of the TCP connection;

means for transmitting the new incoming packet at the first priority if the first priority is not greater than the second priority;

means for determining whether the new incoming packet will arrive substantially out of order in that the incoming packet will arrive before the previous incoming packet such that retransmission of the previous incoming packet or the new incoming packet will result;

means for transmitting the new incoming packet at the first priority if the new incoming packet is not determined to arrive substantially out of order with respect to the previous incoming packet; and

means for transmitting the new incoming packet at the second priority if the new incoming packet is determined to arrive substantially out of order with respect to the previous incoming packet.

57. An article of manufacture having one or more recordable media storing executable instructions thereon which, when executed by a system, cause the system to:

check whether a first priority associated with a new incoming packet of a TCP connection is greater than a second priority associated with a previous incoming packet of the TCP connection;

transmit the new incoming packet at the first priority if the first priority is not greater than the second priority;

determine whether the new incoming packet will arrive substantially out of order in that the incoming packet will arrive before the previous incoming packet such that retransmission of the previous incoming packet or the new incoming packet will result;

transmit the new incoming packet at the first priority if the new incoming packet is not determined to arrive substantially out of order with respect to the previous incoming packet; and

transmit the new incoming packet at the second priority if the new incoming packet is determined to arrive substantially out of order with respect to the previous incoming packet.